A one–parameter family of polynomials with Galois group M_{24} over $\mathbb{Q}(\mathrm{t})$

Peter Müller

March 2, 2013

1 Introduction

Malle and Matzat proved in [3, III.7.5] that the Mathieu group M_{24} is a regular Galois extension of $\mathbb{Q}(t)$. This group was the last sporadic group which could be shown to be a Galois group over the rationals, the only open case remains M_{23}.

The M_{24} Galois extensions $L/\mathbb{Q}(t)$ by Malle and Matzat have the following properties: Let $\mathbb{Q}(t,x)$ be a root field of degree 24 over $\mathbb{Q}(t)$. Then the genus of $\mathbb{Q}(t,x)$ is 0. More precisely, exactly 4 places p_∞, p_0, p_1 and p_2 of $\mathbb{C}(t)$ are ramified in $\mathbb{C}L$. Let P_i be a place in $\mathbb{C}L$ above p_i. Then the inertia group of P_∞ is generated by an element of order 12 with two cycles (in the natural degree 24 action), and each inertia group of P_i, $i = 1, 2, 3$, is generated by an involution with 8 fixed points. Clearly, p_∞ is stable under the absolute Galois group of $\mathbb{Q}$, so p_∞ is rational.

We call a M_{24} Galois extension of $\mathbb{Q}(t)$ (or of $\mathbb{C}(t)$) with this ramification data an extension of type $(12, 2, 2, 2)$.

Malle and Matzat show the following: Up to a natural equivalence, the Galois extensions with the above data, and the added property that p_0 is rational too, are parametrized (up to finitely many exceptions) by the rational curve $\mathbb{P}^1(\mathbb{Q})$. In his thesis [2] Granboulan succeeded to compute an explicit polynomial with these data.

If one requires all branch points p_i to be rational, then the parametrizing curve has genus 1, see [3, III.7.5]. It was left open whether this curve has sufficiently many points to give M_{24} realizations. As a corollary to our computations, we explicitly compute this curve and show that it is an elliptic curve with positive rank. So there are infinitely many M_{24} extension of type $(12, 2, 2, 2)$ with all branch points rational.

The polynomial by Granboulan is somewhat complicated. We believe that there are two reasons for this: First, requiring that p_0 is rational adds a further condition, which rules out most polynomials which could have a nicer shape. Secondly, his polynomial is just a specialization of an unknown one–parametric family, so the kind of random specialization could produce ugly coefficients.

For this reason we computed the whole one–parameter family, and dropped the rationality of p_0.

Theorem. *Let t be a transcendental over $\mathbb{Q}$. For $1 \neq s \in \mathbb{Q}$ let $A_s, B_s \in \mathbb{Q}[X]$ be as in the Appendix. Then the Galois group of $(t - A_s(X))^2 + (X^2+1)B_s(X)^2$ over $\mathbb{Q}(t)$ is* M_{24}.

Remark. For $s = 0$ we get the reasonably sized polynomials

$$\begin{aligned} A_0 = {} & 4194304X^{12} - 72351744X^{10} + 1572864X^9 + 154443776X^8 \\ & - 34062336X^7 + 46684160X^6 + 16098816X^5 - 156060348X^4 \\ & + 30667728X^3 - 5330757X^2 - 3462498X + 9958791 \end{aligned}$$

and

$$\begin{aligned} B_0 = {} & -25165824X^{10} - 1572864X^9 + 145227776X^8 - 16515072X^7 \\ & - 164757504X^6 + 48453120X^5 - 56207872X^4 \\ & - 6865152X^3 + 71415384X^2 - 8906760X + 224829. \end{aligned}$$

In the Theorem, we indeed need to exclude the value $s = 1$. One can show that in this case the Galois group is not doubly transitive, so it is a proper subgroup of M_{24}.

2 Motivation

Let $\mathbb{Q}(t,x)/\mathbb{Q}(t)$ be a $(12,2,2,2)$ extension with branch points p_∞, p_0, p_1, p_2 as in the introduction, such that the normal closure has Galois group M_{24}. Since p_∞ is rational, we may assume that $p_\infty(t) = \infty$. Let k be the residue field of P_∞. Then $[k : \mathbb{Q}] \leq 2$ (actually one can show that k is not real). Then $k(t,x) = k(y)$ (since $\mathbb{Q}(t,x)$ has genus 0 and $k(t,x)$ has a k–rational place). Without loss assume that $y \mapsto 0$ and $y \mapsto \infty$ are the two places above p_∞.

Then

$$t = \frac{g(y)}{y^{12}} = f(y)$$

for $g(Y) \in k[Y]$ of degree 24. Let $a \mapsto \bar{a}$ be the automorphism of kL which is the identity on L and has order 2 on k. From $t = f(y)$ we obtain $t = \bar{t} = \bar{f}(\bar{y})$. On the other hand, $k(\bar{y}) = k(y)$, so

$$\bar{y} = \frac{ay+b}{cy+d}$$

for some $a,b,c,d \in k$. Comparing poles in $\bar{f}(\frac{ay+b}{cy+d}) = f(y)$ shows that either $c = d = 0$ or $a = d = 0$. One can show that the former case cannot hold. Thus $\bar{f}(b/y) = f(y)$. From $y = \bar{\bar{y}} = \bar{b}/\bar{y} = \bar{b}\frac{y}{b}$ we get $\bar{b} = b$, so $b \in \mathbb{Q}$. If $g(Y) = Y^{24} + g_{23}Y^{23} + \cdots + g_1 Y + g_0$, then $b^{12} = g_0$. Thus upon replacing $g(Y)$ with $g(\sqrt{b}Y)/b^{12}$, we may assume that $g(Y)$ is monic with $g_0 = 1$, for the price that we possibly need to replace k by a quadratic extension which we still call k. Note also that $\overline{g_{12}} = g_{12}$.

The ramification over p_0, p_1, p_2 translates to

$$g(Y) - \omega_i Y^{12} = A_i(Y)^2 B_i(Y), \tag{1}$$

where $D(T) = (T - \omega_0)(T - \omega_1)(T - \omega_2) \in k[T]$, and $A_i, B_i \in k[\omega_i][Y]$ are of degree 8.

Generically, the branch points $\omega = \omega_0, \omega_1, \omega_2$ are conjugate over k. Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ with $\omega^{\sigma^i} = \omega_i$. Write $A_0 = U_0 + \omega U_1 + \omega^2 U_2$ with $U_0, U_1, U_2 \in k[Y]$, and similarly $B_0 = V_0 + \omega V_1 + \omega^2 V_2$. Then $A_i = U_0 + \omega_i U_1 + \omega_i^2 U_2$ and $B_i = V_0 + \omega_i V_1 + \omega_i^2 V_2$. By adding a constant to $g(Y)/Y^{12}$ we may assume that $D(T) = (T-\omega_0)(T-\omega_1)(T-\omega_2) = T^3 + pT + q$.

We set up a system of 49 equations for 50 unknowns: The polynomials U_1, U_2, V_1 and V_2 have degree 7, while U_0 and V_0 are monic of degree 8. This gives 48 unknown coefficients. The remaining 2 unknowns are p and q in $D(T) = T^3 + pT + q$.

The 49 equations come from noting that (1) is equivalent to $A_i(Y)^2 B_i(Y) + \omega_i Y^{12}$ being independent of i, that is $(U_0 + \omega U_1 + \omega^2 U_2)^2 (V_0 + \omega V_1 + \omega^2 V_2)$ having all coefficients in k (and constant term 1). Thus treating ω as a variable and reducing the expansion of $(U_0 + \omega U_1 + \omega^2 U_2)^2 (V_0 + \omega V_1 + \omega^2 V_2) + \omega^{12}_Y$ modulo $\omega^3 + p\omega + q$ gives 49 equations.

One can revert the arguments which led to the special shape of $f(Y)$, similar arguments appear in [2]. Suppose that $\bar{f}(Y) = f(\frac{b}{Y})$ with $b \in \mathbb{Q}$. Let y be a root of $f_s(Y) - t$. Set $x = (y + \bar{y})/2$, $z = (y - \bar{y})/2$, so $y = x + z$ with $\bar{x} = x$ and $\bar{z} = -z$. From $f(y) = t$ and $\bar{t} = t$ we get $f(\frac{b}{\bar{y}}) = t$. But y is the single root of $f(Y) - t$ in $k(y)$, so $\frac{b}{\bar{y}} = y$. We get $x^2 + z^2 = y\bar{y} = b$. Next write

$$t = f(y) = \frac{g(x+z)}{(x+z)^{12}} = g(x+z)\frac{(x-z)^{12}}{b^{12}}.$$

Expand the right hand side, and reduce modulo $x^2 + z^2 - b$ with respect to z. This yields $t = A(x) + zB(x)$ for $A, B \in \mathbb{Q}[X]$. Then

$$0 = (t - A(x))^2 - z^2 B(x)^2 = (t - A(x))^2 + (x^2 - b)B(x)^2,$$

so $(t - A(X))^2 + (X^2 - b)B(X)^2$ is a minimal polynomial for x over $\mathbb{Q}(t)$.

3 The Computation

Granboulan gives a single rational function $g(Y)/Y^{12}$ which after adding a constant has the shape as above, with $b = -1$. The fact that all functions $g(Y)/Y^{12}$ with these data and monodromy group M_{24} are parametrized by a rational curve means that the 49 equations in $\mathbb{C}^{50}$ (we cannot fix the at most biquadratic field k, since it could vary with g) describe a rational curve. Furthermore, the coefficients $1 = \gamma_0, \gamma_1, \ldots, \gamma_{23}, \gamma_{24} = 1$ of $g(Y)$ are polynomials in the unknowns we work with. So if we fix a pair $1 \le i < j \le 23$, then the coefficients γ_i and γ_j should be related by a genus 0 curve equation. Using a straightforward Newton iteration and starting from Granboulan's example, we moved in small steps and computed examples of $g(X)$ for $\gamma_{12} = 25, 26, 27, \ldots, 124$ to a very high precision (3000 binary bits). Fix an index $1 \le i \le 22$. Let $(\gamma_{23,j}, \gamma_{i,j})$ be the 100 pairs of the corresponding coefficients. We tried if there is a polynomial relation of total degree m by minimizing $|\sum_{r+s \le m} a_{r,s} \gamma_{23,j}^r \gamma_{i,j}^s|$ subject to $a_{0,0} = 1$ for unknowns $a_{r,s} \in \mathbb{C}$. For the first m which gave a good approximation we used the function `algdep` from the computer algebra package Sage [4] to determine if $a_{r,s}$ can be expected to be algebraic.

To our surprise, it turned out that all the coefficients actually lie in $\mathbb{Q}(i)$ (so k from above is quadratic and does not vary with g), and that each γ_i is a polynomial in the imaginary part of γ_{23}. The family $g_s(Y)$, $s \in \mathbb{C}$, which we obtained fulfills $\overline{f_s}(Y) = f_s(-1/Y)$ for all real s. Now retrieve A_s and B_s from $f_s(Y) = g_s(Y)/Y^{12}$ as described in the previous section. The polynomials A_s and B_s from the appendix slightly differ from those just obtained: The Galois group of $(t-A(X))^2+(1+X^2)B(X)^2$ doesn't change if we multiply A and B by the same nonzero factor from $\mathbb{Q}$, and it does not change if we add an element from $\mathbb{Q}$ to A.

The monic cubic $D(T)$ whose roots are the finite branch points of the splitting field of $(t - A_s(X))^2 + (1 + X^2)B_s(X)^2$ has the form $D(T) = T^3 + p(s)T^2 + q(s)T + r(s)$, where $p, q, r \in \mathbb{Q}[S]$ have degrees 24, 44, and 68, respectively. (Since Sage cannot handle polynomials of large degree, we computed p, q, and r with the help of Magma [1].) Note that by adding a constant to $A(X)$, which amounts to adding the same constant to t, we have given up the original condition that the coefficient of T^2 in $D(T)$ vanishes. If we want to make a branch point p_0 rational, then we need to find a condition on s such that $D(T)$ has a rational root. By Malle–Matzat, the M_{24} extensions with rational p_0 are still parametrized by $\mathbb{P}^1(\mathbb{Q})$. Thus the curve $T^3 + p(S)T + q(S) = 0$ should be a rational curve, so there should be a cubic rational function $S(Z) \in \mathbb{Q}(Z)$ such that $T^3+p(S(Z))T+q(S(Z)) = 0$ has a root in $\mathbb{Q}(Z)$. Let T_0 be a root of $T^3+p(S)T+q(S)$. Working out the ramification of the cubic extension $\mathbb{Q}(S, T_0)/\mathbb{Q}(S)$ allows us to express S in terms of Z, where $\mathbb{Q}(S, T_0) = \mathbb{Q}(Z)$. Indeed, $S(Z) = \frac{(1-2\,Z)\left(9\,Z^2+16\,Z+21\right)}{25\,(Z^2+1)}$.

Eventually, we want to get the condition that all finite branch points are rational. The above parametrization gives a linear factor of $D(T) = T^3 + p(S(Z))T + q(S(Z))$. The square–free part of the discriminant of the quadratic co–factor is $\frac{1}{81}(Z+2)(81\,Z^3+36\,Z^2 + 122\,Z - 2)$. Thus we need to study rational points on the hyperelliptic genus 1 curve $W^2 = \frac{1}{81}(Z + 2)\left(81\,Z^3 + 36\,Z^2 + 122\,Z - 2\right)$. The substitution $Z = \frac{30}{U} - 2$, $W = \frac{50V}{3U^2}$ puts this curve in the Weierstrass form $V^2 = U^3 - 38U^2 + 540U - 2916$. The point $(u, v) = (30, 78)$ is on this curve, but it is not a torsion point by the Nagell–Lutz Theorem (78 does not divide the discriminant of $U^3 - 38U^2 + 540U - 2916$). Thus there are infinitely many M_{24} extensions of $\mathbb{Q}(t)$ of type $(12, 2, 2, 2)$ and all branch points rational. An example is given by $s = 21/25$.

It remains to verify that the polynomials in the Theorem have the correct Galois group. Since M_{24} is self–normalizing in S_{24}, it suffices to show that the given polynomials have Galois group M_{24} over $\mathbb{C}(t)$. Identifying the Galois group with the monodromy group, it is clear that the group does not change if we vary s along a path such that each $F_s(X) = (t - A(X))^2 + (1 + X^2)B(X)^2$ has 4 distinct branch points. Computing the discriminant of $D(T)$ from above gives a high degree polynomial in s whose single rational root is $s = 1$.

Thus it suffices to show that $F_0(X)$ has the correct monodromy group. One checks that $F_0(X)$ is irreducible. If we set $t = 1$ and factor over $\mathbb{F}_7$, we get a linear factor and an irreducible factor of degree 23. By the Dedekind criterion, the Galois group of $F_0(X)$ contains a 23–cycle, so it is doubly transitive. Furthermore, one verifies that the discriminant of F_0 is a square in $\mathbb{Q}[t]$. So the Galois group of F_0 is either M_{24} or

A_{24}. To rule out the latter case, one can numerically compute the four generators of the monodromy group corresponding to four branch points. In a forthcoming paper, we develop an algebraic criterion which bounds the Galois group from above and which is applicable here.

4 Appendix

Here we give the polynomials A_s and B_s from the theorem. These and further polynomials and discriminants, corresponding to p_0 being rational or all p_i rational, appear on the website `www.mathematik.uni-wuerzburg.de/~mueller/Papers/m24.sage` .

$$\begin{aligned}
A_s = {} & 4194304X^{12} + 25165824sX^{11} + (-66060288s^4 - 132120576s^3 + 125829120s^2 \\
& + 157286400s - 72351744)X^{10} + (7864320s^6 - 291766272s^5 - 530055168s^4 \\
& + 374865920s^3 + 589824000s^2 - 257163264s + 1572864)X^9 + (95068160s^8 \\
& + 404160512s^7 - 307265536s^6 - 1711472640s^5 - 319438848s^4 \\
& + 1774780416s^3 + 300646400s^2 - 680329216s + 154443776)X^8 \\
& + (-19660800s^{10} + 245915648s^9 + 1056260096s^8 + 425984s^7 - 2924347392s^6 \\
& - 1609285632s^5 + 2559344640s^4 + 1031438336s^3 - 1117782016s^2 + 308436992s \\
& - 34062336)X^7 + (-24121344s^{12} - 187533312s^{11} + 41097216s^{10} + 1319323648s^9 \\
& + 1257576448s^8 - 1814122496s^7 - 3242037248s^6 - 111439872s^5 + 2190483456s^4 \\
& + 603674624s^3 - 701696000s^2 + 22325248s + 46684160)X^6 + (6127104s^{14} \\
& - 18555136s^{13} - 233881088s^{12} - 175877632s^{11} + 782083584s^{10} + 1554816256s^9 \\
& + 305029632s^8 - 2126697472s^7 - 2687739392s^6 + 342526208s^5 + 2244343296s^4 \\
& + 129376768s^3 - 926989824s^2 + 248273664s + 16098816)X^5 + (750020s^{16} \\
& + 14359744s^{15} + 12053088s^{14} - 114504896s^{13} - 207573520s^{12} - 47353152s^{11} \\
& + 587791264s^{10} + 1525759808s^9 + 817520152s^8 - 2767906752s^7 - 2971570528s^6 \\
& + 2058861504s^5 + 2304495344s^4 - 1478264768s^3 - 673535648s^2 + 730274240s \\
& - 156060348)X^4 + (-240000s^{18} - 771520s^{17} + 4552208s^{16} + 5407552s^{15} \\
& - 12085824s^{14} - 57342016s^{13} - 224008704s^{12} - 145445568s^{11} + 869959872s^{10} \\
& + 1405781568s^9 - 746917472s^8 - 2364491840s^7 + 148282176s^6 + 1768511296s^5 \\
& - 573188480s^4 - 739240000s^3 + 693032896s^2 - 247013248s + 30667728)X^3 \\
& + (8267s^{20} - 60292s^{19} - 189418s^{18} + 387764s^{17} + 49279s^{16} + 10416944s^{15} \\
& + 7799240s^{14} - 96630576s^{13} - 173543962s^{12} + 115412424s^{11} + 495715012s^{10} \\
& + 346585368s^9 - 264331194s^8 - 710757904s^7 - 246179640s^6 + 577521040s^5 \\
& + 203985999s^4 - 432517988s^3 + 97491606s^2 + 11254228s - 5330757)X^2 \\
& + (336s^{22} + 2884s^{21} + 2918s^{20} - 280s^{19} - 187260s^{18} - 551084s^{17} \\
& + 3439942s^{16} + 3990720s^{15} - 13251728s^{14} - 31779288s^{13} - 22616724s^{12} \\
& + 2200016s^{11} + 154829368s^{10} + 220854120s^9 - 178041252s^8 - 448632704s^7 \\
& + 189685920s^6 + 382850836s^5 - 184274706s^4 - 241599992s^3 + 191501284s^2 \\
& - 37543740s - 3462498)X
\end{aligned}$$

$$
\begin{aligned}
B_s = {} & (25165824s^2 + 25165824s - 25165824)X^{10} + (-1572864s^4 + 132120576s^3 \\
& + 116391936s^2 - 119537664s - 1572864)X^9 + (-99614720s^6 - 304349184s^5 \\
& + 268959744s^4 + 804782080s^3 - 132120576s^2 - 452198400s + 145227776)X^8 \\
& + (16711680s^8 - 350552064s^7 - 1014300672s^6 + 369819648s^5 + 2081488896s^4 \\
& - 21430272s^3 - 1230962688s^2 + 417398784s - 16515072)X^7 + (59408384s^{10} \\
& + 340467712s^9 - 186449920s^8 - 1965195264s^7 - 1035206656s^6 + 2817441792s^5 \\
& + 2004549632s^4 - 1769635840s^3 - 729972736s^2 + 797122560s - 164757504)X^6 \\
& + (-13969920s^{12} + 98482176s^{11} + 646695936s^{10} + 245766144s^9 - 2084156928s^8 \\
& - 2286686208s^7 + 2005444608s^6 + 2897768448s^5 - 1126577664s^4 - 1002874880s^3 \\
& + 866995200s^2 - 278562816s + 48453120)X^5 + (-5992448s^{14} - 66636032s^{13} \\
& - 15972864s^{12} + 521017856s^{11} + 692872192s^{10} - 646882048s^9 - 1987540480s^8 \\
& - 873563136s^7 + 1382451200s^6 + 1778852096s^5 - 371893760s^4 - 916518400s^3 \\
& + 335021056s^2 + 142912256s - 56207872)X^4 + (1621440s^{16} + 424640s^{15} \\
& - 47240768s^{14} - 50228288s^{13} + 157415360s^{12} + 409560000s^{11} + 274859712s^{10} \\
& - 417022784s^9 - 1449295296s^8 - 722824128s^7 + 1625973056s^6 + 1180120896s^5 \\
& - 1145317056s^4 - 494068416s^3 + 737746496s^2 - 163911616s - 6865152)X^3 \\
& + (5000s^{18} + 1616880s^{17} + 2639064s^{16} - 12017344s^{15} - 21008416s^{14} \\
& - 17153152s^{13} + 56032160s^{12} + 274166336s^{11} + 340729008s^{10} - 518906656s^9 \\
& - 1093524848s^8 + 245942208s^7 + 1311410912s^6 - 338458624s^5 - 772161888s^4 \\
& + 347966656s^3 + 363724040s^2 - 309525584s + 71415384)X^2 + (-16656s^{20} \\
& - 101144s^{19} + 120440s^{18} + 90968s^{17} - 360488s^{16} - 1152768s^{15} - 16231616s^{14} \\
& - 20363328s^{13} + 68279648s^{12} + 152960784s^{11} - 28705040s^{10} - 273001168s^9 \\
& - 97695248s^8 + 225560384s^7 + 24231552s^6 - 162720512s^5 + 97096176s^4 \\
& + 102722504s^3 - 152893224s^2 + 65919672s - 8906760)X + 527s^{22} + 1138s^{21} \\
& - 549s^{20} - 1556s^{19} - 32451s^{18} + 372274s^{17} + 599009s^{16} - 2859792s^{15} \\
& - 6690746s^{14} + 2971140s^{13} + 16373566s^{12} + 15848168s^{11} + 5309674s^{10} \\
& - 29793004s^9 - 62702414s^8 + 18214832s^7 + 82023963s^6 - 11931446s^5 \\
& - 56636393s^4 + 22914700s^3 + 5802345s^2 - 4202118s + 224829
\end{aligned}
$$

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Louis Granboulan. Construction d'une extension régulière de $\mathbf{Q}(T)$ de groupe de Galois M_{24}. *Experiment. Math.*, 5(1):3–14, 1996.

[3] G. Malle and B. H. Matzat. *Inverse Galois Theory.* Springer Verlag, Berlin, 1999.

[4] W. A. Stein et al. *Sage Mathematics Software (Version 4.8).* The Sage Development Team, 2012. `http://www.sagemath.org`.